

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case No.23-1816M(NJ)  
Information associated with Apple IDs: ) **Matter No. 2022R00505**  
randj15@icloud.com and jmtimecorp@icloud.com, stored )  
by Apple, Inc., as further described in Attachment A )

**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before 10/27/2023 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

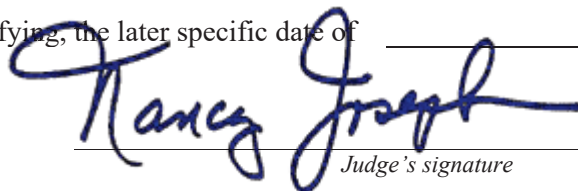
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to \_\_\_\_\_

Hon. Nancy Joseph  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 10/13/2023 @ 3:45 p.m.

  
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

## Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

---

*Executing officer's signature*

---

*Printed name and title*

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

**Account 1:** [randj15@icloud.com](mailto:randj15@icloud.com); and

**Account 2:** [jmtimecorp@icloud.com](mailto:jmtimecorp@icloud.com)

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 1, 2021, through October 10, 2023, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. All The contents of all instant messages associated with the account from January 1, 2021, through October 10, 2023, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. All The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks associated with the account from January 1, 2021, through October 10, 2023;

f. All activity, connection, and transactional logs for the account (with associated IP

addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades associated with the account from January 1, 2021, through October 10, 2023;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps associated with the account from January 1, 2021, through October 10, 2023;

h. All records pertaining to the types of service used;

a. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

## **II. Information to Be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 21, United States Code, Sections 846 and 841(a)(1)

(conspiracy to distribute cocaine and distribution of cocaine) and money laundering statutes of Title 18, United States Code, Sections 1956 (a)(1)(B)(i) knowingly conducting or attempting to conduct, a financial transaction with proceeds from specified unlawful activity with specific intent to: Conceal the nature, source, location, ownership, or control of proceeds and 1956 (h) Money Laundering Conspiracy, those violations involving John MARIN since January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

- a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of WisconsinIn the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

Case No.23-1816M(NJ)

Information associated with Apple IDs:  
randj15@icloud.com and jmtimecorp@icloud.com  
stored by Apple, Inc., as further described in Attachment A**Matter No. 2022R00505****APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 841(a)(1) & 846	Distribution and conspiracy to distribute cocaine.
18 U.S.C. § 1956	Money laundering.

The application is based on these facts:

See Attached Affidavit.

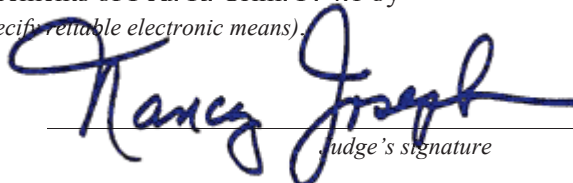
☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days *(give exact ending date if more than 30 days: \_\_\_\_\_)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.**CURT R HANSEN**Digitally signed by CURT R HANSEN  
Date: 2023.10.12 17:06:05 -05'00'*Applicant's signature*

Curt Hansen, HSI SA

*Printed name and title*Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ *(specify reliable electronic means)*.

Date: 10/13/2023

City and state: Milwaukee, WI


*Judge's signature*

Honorable Nancy Joseph, U.S. Magistrate Judge

*Printed name and title*



**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, HSI Special Agent Curt Hansen, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the Apple IDs and Apple iCloud accounts associated with the following information, further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California 95014:

**Account 1: [randj15@icloud.com](mailto:randj15@icloud.com); and**

**Account 2: [jmtimecorp@icloud.com](mailto:jmtimecorp@icloud.com)**

2. I am a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Resident Agent in Charge (RAC) Milwaukee, Wisconsin. I have been employed with HSI as a Special Agent for approximately two years. Prior to employment with HSI, I worked as a Deputy United States Marshal, Federal Air Marshal, and United States Border Patrol Agent. I have been a sworn federal law enforcement officer specifically investigating crimes involving narcotics, firearms, smuggling, terrorism, and immigration since September 2011. Throughout my law enforcement career, I have received training in general law enforcement and in specialized areas including narcotics and human smuggling. I am an investigator or law enforcement officer of the United States within the meaning of Title 8, United States Code, Section 1357(a)(5), that is, an officer of the

United States who is empowered to conduct investigations of, and to make arrests for, certain offenses enumerated in Titles 8, 18, 19, 21, and 31 of the United States Code, and other related offenses. Since becoming employed as a federal agent, I have completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Brunswick, Georgia. As part of my duties and responsibilities as an HSI Special Agent, I am authorized to investigate crimes that involve narcotics violations pursuant to Title 21, United States Code.

3. As part of my duties as an HSI Special Agent, I have experience conducting criminal investigations involving narcotics, firearms, gangs, and human smuggling and have participated in the execution of search warrants in such investigations. I am familiar with various methods of smuggling and trafficking narcotics and other controlled substances and the proceeds from sale of such substances. I am also familiar with methods used to evade detection of both the controlled substances and the proceeds from their sale that are used by drug traffickers.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Throughout this affidavit, reference will be made to case agents or investigators. Case agents or investigators are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your Affiant has had regular contact regarding this investigation.

#### **PURPOSE OF AFFIDAVIT**

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 846 and 841(a)(1) (conspiracy to distribute cocaine and distribution of cocaine) and Title 18, United States Code, Sections 1956 and

1956(h)(money laundering and money laundering conspiracy) have been committed, are being committed, or will be committed by John Marin, and others and that there is probable cause to believe that the Apple iCloud Accounts, described in Attachment A, contain evidence of violations of Title 21, United States Code, Sections 846 and 841(a)(1) (conspiracy to distribute cocaine and distribution of cocaine) and Title 18, United States Code, Sections 1956 and 1956(h) (money laundering and money laundering conspiracy), as described in Attachment B.

6. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated; *see* 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **A. Wisconsin Search Warrant**

7. In August 2022, HSI Milwaukee, Milwaukee Police Department Violent Crimes Unit (MPDVCU), along with members of DEA Group 68 initiated an investigation into individuals distributing cocaine throughout Milwaukee, Wisconsin. HSI identified the individuals involved in this cocaine drug trafficking as, among others, Antonio LONG, Brian WILBERT, John MARIN, and Bobby PERRY.

8. On August 9, 2022, Milwaukee Police Department Violent Crimes Unit (MPDVCU) District 3 executed a Wisconsin State search warrant at 5709 North 78th Street, Milwaukee, Wisconsin. During the search of the residence, MPDVCU located and seized crack cocaine, marijuana, psilocybin, two handguns (Glock 19 and Sig P365), various ammunition with high-capacity magazines, high dollar jewelry items, approximately \$10,076 in US currency, and various scales with narcotic residue on them as well as other narcotics-related paraphernalia.

A black Samsung smartphone was also seized. MPDVCU seized bank documents and invoices that displayed large currency transactions for jewelry, automobiles, and transfers of currency. Among documents seized, an invoice with the business name “Buck Eyes” was seized. Based on their training and experience, and the investigation to date, case agents believe the invoice is narcotics related. Finally, seized documents indicated that the target for the search warrant had a storage unit at W135N8945 Wisconsin 145, Menomonee Falls, Wisconsin in Waukesha County, Wisconsin.

9. That same day, MPDVCU applied for and obtained an additional search warrant for storage unit number 515 at W135N8945 Wisconsin 145, Menomonee Falls, Wisconsin. During the search of the storage unit, MPDVCU located 21 clear corner cut plastic baggies containing cocaine and five pressed bricks of a cocaine. A combined total of 5.8 kilograms of cocaine was present. MPDVCU also recovered 20 large vacuum sealable plastic bags containing marijuana with a total weight of 18.7 pounds. A .9mm Palmetto State Armory AR-15 (AR Pistol) and a Maverick model 88 12-gauge shotgun with sawed off barrel were located within the storage unit. Finally, MPDVCU seized approximately \$39,610 in US currency from the unit.

10. On August 18, 2022, the MPDVCU requested assistance from HSI Milwaukee and DEA Group 68 to assist with the investigation. Through information obtained from a confidential source (CS #1), historical law enforcement records, electronic surveillance, toll record analysis, social media exploitation, and open-source databases, HSI Special Agents and MPDVCU determined the source of supply for the cocaine that was seized is the Antonio LONG drug trafficking organization (DTO). This DTO is headed by LONG, who orchestrates the distribution of kilogram quantities of cocaine across the state of Wisconsin. Investigators have determined that LONG and his DTO obtain and distribute as many as 30 kilograms of cocaine

monthly to the Milwaukee, Wisconsin area.

11. For several reasons, case agents believe that CS #1 is reliable and credible. First, CS #1 has been providing information since August of 2022. Second, the information provided by CS #1 is consistent with evidence obtained elsewhere in this investigation where CS #1 was not utilized, and substantial portions of CS #1's information has been corroborated through independent investigation. CS #1 is cooperating for consideration on state drug trafficking charges. CS #1 has prior felony convictions for robbery and a weapons violation. Finally, CS #1 has had an adequate opportunity to directly observe the events discussed and/or has heard conversations directly from the individuals discussed herein. For these reasons, case agents believe CS #1 to be reliable.

**B. Historical Information About LONG's Drug-Trafficking From CS#1**

12. CS #1 told case agents that the cocaine is transported via a white Ford Transit van concealed in furniture or within a trap built into the vehicle's floor. The white Ford Transit van bearing Arizona license plate number Z6A6CAA is registered to Brian WILBERT. CS #1 stated that WILBERT is the primary source of transportation for the LONG DTO. WILBERT is the cousin of LONG and has a residence in Gilbert, Arizona. CS #1 stated that upon receipt of the cocaine, the LONG DTO sells the cocaine by the kilogram, frequently making multiple kilogram sales per customer. The LONG DTO has been actively operating in the Milwaukee area for approximately five years.

13. CS #1 stated that she/he regularly communicates with WILBERT through cellular telephones to coordinate delivery of narcotics over the past five years. WILBERT would contact CS #1 to coordinate the "drop" of cocaine and marijuana. Shipments of cocaine and marijuana were delivered to locations in Milwaukee, Wisconsin monthly and on several occasions biweekly

for over five years. Throughout the duration of the shipment, CS #1, WILBERT, and LONG would maintain contact to ensure delivery of the narcotics.

14. On September 7, 2022, HSI and DEA Group 68 conducted a forensic analysis of the cellular telephone that was seized from the search warrant conducted at 5709 North 78th Street, Milwaukee, Wisconsin. A review of the SMS text messages revealed conversations between CS #1 and LONG. The text thread covered a period of four months and detailed conversations between CS #1 and LONG discussing the transportation and sale of narcotics. LONG frequently sent text messages highlighting when shipments, transported by WILBERT, of cocaine and marijuana were to be sent to CS #1. LONG regularly discussed the need to deliver more kilograms of cocaine and would also notify CS #1 when packages of the narcotics proceeds were to be sent back to Los Angeles, California. The text messages indicate that LONG supplies and directs the shipments of cocaine.

15. CS #1 stated the proceeds from narcotics sales are collected by CS #1 and mailed via FedEx. Listed on the shipping contents of the package are high-dollar jewelry items, for example Rolex watches. CS #1 has acknowledged to have mailed upwards of \$275,000 at one time. LONG emails CS #1 invoices stating how much payment are due for the cocaine. The invoices have jewelry listed as the purchase item along with the fee listed for them. Case agents viewed the emails provided by CS #1. LONG is listed as the sender and the email address is illdreams88@gmail.com. CS #1 received an invoice from LONG approximately every week from LONG's email address. The invoices purport to be from the following businesses listed: JM Time Corp., Virgo Stones Jewelry Company, Ortho Lab, International Players Club Inc. (also IPC Jewelry), and Prestige Fine Metals. Open records check on the above listed businesses indicate that JM Time Corp is a registered limited liability corporation with the state of

California associated with MARIN. Ortho Labs and Virgo Stones Jewelry do not have an official registration with the state of California or any other official entity making them legitimate businesses, however, based on FedEx shipping labels indicate they are associated with MARIN and GONZALEZ CRUZ. International Players Club Inc and Prestige Fine Metals also do not have any official registration with the state of California or any other official entity making them legitimate businesses, shipping labels indicate that International Players Club is associated with Michael ALEMAN and Prestige Fine Metals is associated with Michelle SABRA.

16. CS #1 detailed how “jewelry” and jewelry-related terms are used as code words for the cocaine on the invoices to give the impression of a legitimate business transaction. After receiving invoices via email, CS #1 packaged currency in FedEx boxes with a preprinted shipping label, which s/he received from LONG. Since 2021, the recipient listed on the preprinted shipping labels was listed as John MARIN. According to database and record checks, MARIN is listed as the owner of JM Time Corporation, Virgo Stones and Jewelry Company, and Ortho Lab. CS #1 admitted to taking the packages to FedEx mailing facilities in the greater Milwaukee area and mailing them priority overnight to locations in California, primarily the Los Angeles area.

**C. Search of LONG’s Arizona Residence**

17. On January 26, 2023, HSI Milwaukee and HSI Casa Grande executed a federal search warrant at 2888 S. Beckett Street, Gilbert, Arizona, which is associated with Antonio LONG. HSI seized seven cellular telephones and two iPads from the residence and conducted a forensic examination of the devices. Case agents reviewed each forensic examination conducted to preserve any evidence. Notably, within the black iPad and two LG phones of the seizure,

Case agents discovered preprinted shipping labels and invoices saved within the devices in the form of images and documents. These images were created and delivered via email and saved to LONG's devices before being emailed, using bucksmke36@gmail.com and illdreams88@gmail.com, to the distributors in the Milwaukee area. The preprinted shipping labels are the same type of labels encountered previously in the investigation. The shipper and receiver listed on the labels are MARIN and others listed in the investigation; the sending and receiving addresses are both locations in Los Angeles, California and are businesses owned by MARIN.

18. The invoices located on the devices were from a purported business called "Buck Eyes" with telephone number (323) 497-4868 and email address bucksmke36@gmail.com. In the body of the invoice there are names that appear to be names of narcotic types and opposite of the names are prices of the narcotics by the pound. The invoices located on the device are the same type of invoices found in the residence at 5709 North 78th Street, Milwaukee, Wisconsin. The invoices sent to LONG's email from bucksmke36@gmail.com, the email associated with the seized devices, indicates a date timeframe between February 2019 through January 2023. The phone number (323) 497-4868 listed on the invoice was queried against databases and was previously identified as one of the phone numbers belonging to LONG.

19. Following the search of LONG's residence in Arizona, LONG was advised of and waived his rights. LONG spoke to case agents about his cocaine and marijuana distribution. LONG confirmed that he would order shipments of narcotics from MARIN and have WILBERT transport the narcotics to locations in the greater Milwaukee, Wisconsin area. During the interview, LONG stated that the proceeds of the narcotics sales were packaged in FedEx Express packages and shipped to MARIN and others in Los Angeles, California. LONG also



acknowledged that he would receive preprinted shipping labels and invoices from MARIN and others and email them using illdreams88@gmail.com and bucksmke36@gmail.com to narcotics distributors in Wisconsin. LONG was asked why the proceeds did not go to him directly, LONG stated “everyone sent all the money to John (MARIN) because he has a system, the coke and the weed money went to him.” “John (MARIN) has a system,” LONG also stated.

20. CS #1 was consulted by case agents about the invoices and shipping labels. CS #1 explained that the invoices for “Buck Eyes” are from LONG. CS #1 explained to agents that s/he would receive those invoices from LONG for marijuana orders/purchases. S/he stated that “Buck Eyes” is LONG’s marijuana venture. CS #1 said that s/he received invoices since the beginning when s/he was selling narcotics for the DTO. CS #1 explained that at the start of the DTO, LONG was selling marijuana. S/he said that LONG contacted suppliers in California and the suppliers would front the marijuana to LONG. LONG took orders from dealers in various locations within the US and coordinated the shipment of the marijuana to the dealers, via mail or vehicle. CS #1 stated that first s/he received marijuana in the mail, but after the DTO got more business and orders became larger, LONG employed Brian WILBERT to transport the narcotics. CS #1 also stated that LONG used “Buck Eyes” invoices in order to differentiate between marijuana and cocaine proceeds. CS #1 stated that when bulk cash was shipped via FedEx, the money was packaged in three layers. The first layer had the bulk cash in a smaller box/envelope, the second layer contained the packaged cash box/envelope placed into a medium box with an invoice, the third layer contained all previous contents placed in a larger box that was sealed. The exterior of the third box would have the preprinted shipping label affixed to it and would be shipped FedEx Express.

21. CS #1 explained that after she/he received the narcotics, LONG emailed an invoice from both illdreams88@gmail.com and bucksmke36@gmail.com with a shipping label. CS #1 said the invoices would indicate how much money was to be sent via FedEx back to California. CS #1 stated that all the proceeds were mailed via FedEx and the proceeds were always sent to locations in the greater Los Angeles, California area. CS #1 stated that the recipient was typically John MARIN but that other recipients were used frequently (Fernando TALLEY, Michael ALEMAN, Graciela GONZELEZ-CRUZ, Michelle SABRA, and others). CS #1 stated that s/he mailed several hundred thousand dollars per month in proceeds based on the “Buck Eyes” invoices.

**D. Search of Bobby Perry’s Wisconsin Residence**

22. On January 26, 2023, HSI Milwaukee executed a federal search warrant at 3710 W. Good Hope Road in Milwaukee, Wisconsin which is associated with Bobby PERRY. HSI seized several electronic devices including cellular telephones and computers. Forensic examination of the devices revealed shipping labels and Buck Eyes invoices similar to those recovered earlier in the investigation. Case agents recovered multiple text threads discussing the purchase and sale of narcotics in PERRY’s phone. The dates listed on the invoices and text threads cover the time between October 2022 and January 2023. Review of all devices from the search warrants reveal that LONG is brokering the distribution of cocaine and marijuana from Los Angeles, California to Milwaukee, Wisconsin, and additional locations within the United States. LONG uses the purported business “Buck Eyes” and bucksmke36@gmail.com and illdreams88@gmail.com to facilitate the shipment of narcotics and their proceeds. LONG, using bucksmke36@gmail.com and illdreams88@gmail.com, received the invoices and shipping labels from MARIN with no text or body in the email, which he then forwarded to recipients in the

Milwaukee area, from this specific forensic examination the emails were sent to PERRY.

23. On June 26, 2023, case agents subpoenaed obtained FedEx Express records for packages shipped and received to MARIN and his businesses. While reviewing the returns from the subpoena, case agents observed that both MARIN and GONZALEZ CRUZ were receiving packages regularly throughout 2023. Case agents noted that both MARIN and GONZALEZ CRUZ received packages days before the subpoena through (conclusion) date. The packages were all listed with MARIN being the sender and receiver on the shipping label. All packages had the same dimensions and restrictions as previous packages that were sent with bulk cash. Based on their training and experience and the investigation to date, case agents believe that the organization is still receiving bulk cash packages via FedEx Express.

**E. Arrest of Brian Wilbert and Recovery of Narcotics**

24. On October 19, 2022, law enforcement obtained a search warrant for the location of Wilbert's 2019 White Ford Transit Van, bearing Arizona license plate number Z6A6CAA. On November 21, 2022, at approximately 9:00 AM, the Waukesha County Drug Group stopped Wilbert's white Ford van on Interstate 43 near the city of Mukwonago, Wisconsin. This area is in the southeastern corner of Waukesha County, Wisconsin within the Eastern District of Wisconsin. A K9 alerted to the presence of narcotics in the vehicle and the vehicle was later searched. The search yielded 3.7 kilograms of cocaine/fentanyl mix, 23.22 kilograms of marijuana, and 889 grams of psilocybin. All items were seized, and Wilbert was taken into custody.

25. On November 21, 2022, after being advised of and waiving his rights, Wilbert admitted that he drove to Los Angeles on November 18, 2022, where he contacted a man named "Red," who owns jewelry stores in the area. Wilbert identified John Marin by photograph and as

the same individual he knows as “Red.” Wilbert stated that he picked up cocaine at a jewelry store at 831 S. Olive Street. Wilbert stated that the jewelry store at 831 S. Olive Street is owned by Marin and is called JM Time Corp. Wilbert stated that he transports cocaine for Marin and has been doing so for the past three years. Wilbert stated he contacts Marin by using WhatsApp and showed case agents a text thread in WhatsApp between Wilbert and Marin. Case agents viewed the text thread in which Marin gave Wilbert instructions on when and how to pick-up cocaine at JM Time Corp. Wilbert stated when he stopped in front of JM Time Corp., Marin’s assistant walked out of the jewelry store carrying a medium-sized black tote with a yellow lid. Wilbert said the assistant put the tote in Wilbert’s van and walked back to the jewelry store. Wilbert said every time he has picked up narcotics from Marin, the assistant always brought out the narcotics and the narcotics were always in the exact same type of tote. Notably, the cocaine/fentanyl located in Wilbert’s van on November 21, 2022, was stored inside a medium-sized black tote with a yellow lid.

26. Wilbert stated after he received the cocaine from Marin during the November 2022 trip, Wilbert drove south to Gardena, California. Wilbert said he stopped at a warehouse at the address of 1223 W. El Segundo Blvd, Gardena, CA. He stated the address was where an unknown man named “C” told him to go to pick up a load of marijuana. Wilbert stated he was there for about an hour while a group of men canned and loaded marijuana in his van. The marijuana located in Wilbert’s van on November 21, 2022, was stored in large aluminum cans that were sealed. Wilbert stated that after the marijuana was loaded into his van, he left the area and began driving toward Wisconsin.

27. Wilbert claimed he was going to drive to Milwaukee, Wisconsin to meet “BJ” to deliver the narcotics load. Wilbert was shown a photograph of Bobby Perry, a subject identified

though this investigation as being one of the Milwaukee area distributors for this DTO. Wilbert identified the photograph of Bobby Perry as “BJ.” Wilbert stated that he was going to deliver the narcotics to Perry’s residence located at 3710 W. Good Hope Road, Milwaukee, Wisconsin. Wisconsin utility records list has Perry as the owner of 3710 W. Good Hope Road. Wilbert stated that for years, he has delivered narcotics to Perry and to Perry’s residence. Wilbert said that Perry, Long, CS #1, and Wilbert would coordinate cocaine shipments multiple times per month and have done so for over three years.

28. Wilbert stated that Long is the broker for all of the narcotics shipments for the past four to five years. Wilbert stated Long is in contact with Marin and “C.” Wilbert stated Long will contact Marin and “C” to negotiate narcotics shipments to Milwaukee, Wisconsin. After Long has contacted Marin and “C,” Long will contact Wilbert to determine which shipments Wilbert will transport. Wilbert stated that he generally gets paid \$4,000 to transport the shipments and is paid in California before he begins the trip. Wilbert stated that, in the past, he has transported narcotics provided by Marin to other locations across the United States at Long’s direction. Wilbert also gave the phone numbers for Marin (WhatsApp) 949-566-3812 and Long 323-523-3432. The phone numbers provided have been identified as Marin and Long’s phone numbers based on investigative findings and tolls analysis conducted by case agents.

#### **F. Review of Financial Records**

29. Financial account records were obtained from JPMorgan Chase Bank for the period beginning January 1, 2016, through December 15, 2022. Those records revealed that John MARIN is a signatory on the following deposit accounts:

Account Name	Account #	Date Opened	Latest Statement
--------------	-----------	-------------	------------------

Marin, John	*3650	05/01/2014	12/15/2022
Marin, John & Ana	*5920	02/29/2020	12/15/2022
Marin, John & Ana	*0323	12/26/2013	12/16/2021
Marin, John & Chris	*0331	12/26/2013	08/18/2020
JM Time Corp	*6852	05/07/2014	11/30/2022
EMJ Wholesale, LLC	*2308	06/15/2018	12/02/2019
EMJ Wholesale, LLC	*3610	<b>03/17/2022</b>	11/30/2022
<b>R&amp;J Basketball, LLC<sup>1</sup></b>	*3839	<b>03/17/2022</b>	11/30/2022
<b>R&amp;J Exotics, LLC</b>	*2090	<b>03/17/2022</b>	11/30/2022
Sector Records, LLC	*0955	<b>03/17/2022</b>	11/30/2022

30. Based on their training and experience, and the investigation to date, case agents believes that analysis of Marin's JPMorgan Chase Bank account records reveals evidence of probable money laundering and potential income tax evasion. With respect to JM Time Corp., this account conducted the majority of transactions, including many potentially legitimate jewelry wholesale transactions. Based on their training and experience, and the investigation to date, case agents believe that Marin used JP Morgan x6852 to disguise his drug proceeds as income from JM Time Corp's jewelry business. Analysis of this account revealed the following:

---

<sup>1</sup> Although the California Secretary of State's Office website failed to identify any businesses associated with John Marin that included "R&J" in the business name, two bank accounts associated with Marin do include those initials. They are bolded in this table. Of note, the FedEx shipping labels sent to CS #1 were sometimes addressed to business names that included "R & J."

- During the 19-months from May 2021 through November 2022, \$807,360 in U.S. currency was deposited into JM's account.
- Most of those currency deposits corresponded with transfers to Marin's family members, either directly or through the payment of their personal expenses.
- Payments (17) against Julieana Munoz's (John Marin's wife) American Express credit card balances, totaling \$260,649.18;
- Zelle payments (6) to Julieana Munoz, totaling \$14,800.00;
- Transfers (7) to John Marin's personal checking account, totaling \$31,400.00;
- Payments (3) against John Marin's Chase Bank card, totaling \$25,891.44;
- Transfers (2) to John Marin's EMJ Wholesale, LLC bank account, totaling \$7,000.00;
- Transfers (2) to John Marin's R&J Exotics, LLC bank account, totaling \$6,500.00;
- Transfers (1) to John Marin's Sector Records, LLC bank account, totaling \$21,000.00; and
- A payment to Ronnel P. Panopio, totaling \$9,600.00.
- Credits into JM Time Corp's account also included the following totals from John Marin's suspected illegal drug trafficking associates:
 

1)	Antonio Long	\$ 5,000
2)	Carlos Ferreira	\$ 12,200
3)	Michael Aleman	\$ 1,500
4)	Ronnel Panopio	\$ 42,179

**G. John Marin's iCloud accounts**

31. MARIN, who resides in Mission Viejo, California, has been illegally operating a cocaine and marijuana drug trafficking organization that has provided monthly amounts of up to 30 kilograms of cocaine and large quantities of marijuana to large-scale distributors in the Milwaukee, Wisconsin area for the past five years. MARIN then disguises the drug payments received from his Milwaukee distributors as payments for purchases of jewelry from one of MARIN's businesses. This money laundering scheme is accomplished by MARIN providing his drug distributors with an invoice from one of his businesses

that indicates an amount owed for jewelry, which is an actual amount owed for the illegal drugs provided by MARIN. MARIN also provides his distributors with a FedEx shipping label, which is used by MARIN's drug distributors to send the invoice and the amount owed, in the form of currency, to MARIN. Most of the FedEx shipping labels further disguised the source of the currency by stating that the container was shipped from John MARIN, of the business named "R&J", at 631 S. Olive Street, Suite 202, Los Angeles, CA to John Marin, of the business named "Ortho Lab", at 959 E. Walnut Street, Pasadena, CA. Additionally, evidence has been gathered that indicates that MARIN has realized substantial cash income from his drug trafficking. The evidence to date further indicates that MARIN has engaged in various money laundering efforts, including the use of his jewelry-related businesses to disguise the cash income from drug trafficking. Toll analysis of MARIN's cellphone number indicates that he is in regular contact with most suspects listed in the affidavit on a daily basis by means of WhatsApp voice and messaging. To date, MARIN has maintained his WhatsApp communications with all targets of the investigation. MARIN routinely utilizes his cellular phone to contact targets of this investigation, primarily through means of end-to-end encryption applications.

32. On June 26, 2023, case agents subpoenaed FedEx Express records for packages shipped to and/or received by MARIN and his businesses. While reviewing the returns from the subpoena, case agents observed that both MARIN and GONZALEZ CRUZ were receiving packages regularly throughout 2023. The packages were all listed with MARIN being the sender and receiver on the shipping label. All packages had the same dimensions and restrictions as previous packages that were sent with bulk cash. Based on their training and experience and the investigation to date, case agents believe that the organization is still receiving bulk cash packages via FedEx Express.

33. According to records from Apple, MARIN is the listed subscriber for **randj15@icloud.com** and **jmtimecorp@icloud.com**. During an interview with law enforcement, LONG admitted to trafficking cocaine with MARIN and to using encryption apps



and messages on his cellular telephone to facilitate and monitor narcotics trafficking. LONG further admitted that he regularly sent MARIN electronic payments for narcotics. Review of iMessages corroborates LONG. For example, case agents located iMessages from Rafael PONCE (MARIN's assistant) instructing LONG to send payments to the **randj15@icloud.com** account. As another example, case agents located an iMessage in which LONG instructed his daughter, Shaylyn LONG, to send payments to **randj15@icloud.com**. Case agents are aware that Apple permits payments to be sent to iCloud accounts via a service called Apple Pay. Based on their training and experience, and the investigation to date, case agents believe that the payments sent from PONCE and Shaylyn LONG to **randj15@icloud.com** were for narcotics provided by MARIN.

34. Case agents are aware that MARIN has two cellular telephone numbers. Analysis of MARIN's Phone numbers for a one-year period reflect that there are almost three times as many calls as there are text messages. Based on their training and experience, and the investigation to date, case agents believe that MARIN primarily uses iMessages to communicate, which are not visible on toll records. Affiant is aware from a review of data located on LONG's cellphone that MARIN communicates using iMessage. LONG has MARIN's cellular numbers stored in his device and the **randj15@icloud.com** account. Further inspection of LONG's device revealed that MARIN and LONG had numerous Facetime calls between October 2022 and December 2022. It is known to case agents that Apple iPhones are set up to automatically save iMessages and Facetime content to iCloud. It is also known to case agents that MARIN and members of his DTO are regularly utilizing iMessage, Facetime, and encrypted applications to avoid detection by law enforcement and to further their criminal conduct.

35. According to records from JP Morgan, **randj15@icloud.com** is linked to

MARIN's bank account ending in x6852 (JM Time Corp). Based on a review of Marin's financial records, the JP Morgan account x6852 was used to conduct the majority of the transactions for JM Time Corp. Based on their training and experience, and the investigation to date, case agents believe that MARIN used JP Morgan x6852 to disguise his drug proceeds as income from JM Time Corp's jewelry business.

36. Based on their training and experience, and the investigation to date, case agents believe that MARIN continues to distribute large amounts of cocaine and launder the proceeds of narcotic sales. MARIN also continues to utilize Apple platforms, including **randj15@icloud.com** and **jmtimecorp@icloud.com**, iCloud, iMessage, and FaceTime to communicate with others regarding the drug trafficking and money laundering activities of the DTO. Case agents are aware that accounts linked to @icloud.com, including **randj15@icloud.com** and **jmtimecorp@icloud.com**, are backed up and stored within iCloud, thus providing the account holder quick access and additional storage of their accounts. Case agents believe the receipt of additional information from Apple pursuant to this search warrant will further the investigation and assist with: the identification of additional locations used by the MARIN to receive, store, and distribute cocaine; the identification of other co-conspirators who distribute cocaine and/or assist in the laundering of drug proceeds for the DTO; and the identification of methods used by DTO members to communicate regarding the drug trafficking and money laundering methods of the DTO.

#### **AUTHORIZATION REQUEST**

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

**Account 1: [randj15@icloud.com](mailto:randj15@icloud.com); and**

**Account 2: [jmtimecorp@icloud.com](mailto:jmtimecorp@icloud.com)**

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 1, 2021, through October 10, 2023, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. All The contents of all instant messages associated with the account from January 1, 2021, through October 10, 2023, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. All The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks associated with the account from January 1, 2021, through October 10, 2023;

f. All activity, connection, and transactional logs for the account (with associated IP

addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades associated with the account from January 1, 2021, through October 10, 2023;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps associated with the account from January 1, 2021, through October 10, 2023;

h. All records pertaining to the types of service used;

a. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

## **II. Information to Be Seized by the Government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 21, United States Code, Sections 846 and 841(a)(1)

(conspiracy to distribute cocaine and distribution of cocaine) and money laundering statutes of Title 18, United States Code, Sections 1956 (a)(1)(B)(i) knowingly conducting or attempting to conduct, a financial transaction with proceeds from specified unlawful activity with specific intent to: Conceal the nature, source, location, ownership, or control of proceeds and 1956 (h) Money Laundering Conspiracy, those violations involving John MARIN since January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

- a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- d. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of \_\_\_\_\_.

\_\_\_\_\_.

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature